Received 17 June 2015
Revised 31 August 2015
25 October 2015
Accepted 25 October 2015

Why don't UK citizens protest against privacy-invading dragnet surveillance?

Karen Renaud
School of Computing Science, University of Glasgow, Glasgow, UK
Stephen Flowerday
Department of Information Systems, University of Fort Hare, East London, South Africa
Rosanne English
School of Computing Science, University of Glasgow, Glasgow, UK, and
Melanie Volkamer
Fachbereich Informatik, TU Darmstadt, Darmstadt, Germany

Abstract

Purpose – The purpose of this study was to identify to identify reasons for the lack of protest against dragnet surveillance in the UK. As part of this investigation, a study was carried out to gauge the understanding of "privacy" and "confidentiality" by the well-informed.

Design/methodology/approach – To perform a best-case study, the authors identified a group of well-informed participants in terms of security. To gain insights into their privacy-related mental models, they were asked first to define the three core terms and then to identify the scenarios. Then, the participants were provided with privacy-related scenarios and were asked to demonstrate their understanding by classifying the scenarios and identifying violations.

Findings – Although the participants were mostly able to identify privacy and confidentiality scenarios, they experienced difficulties in articulating the actual meaning of the terms privacy, confidentiality and security.

Research limitations/implications – There were a limited number of participants, yet the findings are interesting and justify further investigation. The implications, even of this initial study, are significant in that if citizens' privacy rights are being violated and they did not seem to know how to protest this and if indeed they had the desire to do so.

Practical implications – Had the citizens understood the meaning of privacy, and their ancient right thereto, which is enshrined in law, their response to the Snowden revelations about ongoing wide-scale surveillance might well have been more strident and insistent.

Originality/value – People in the UK, where this study was carried out, do not seem to protest the privacy invasion effected by dragnet surveillance with any verve. The authors identify a number of possible reasons for this from the literature. One possible explanation is that people do not understand privacy. Thus, this study posits that privacy is unusual in that understanding does not seem to align with the ability to articulate the rights to privacy and their disapproval of such widespread surveillance. This seems to make protests unlikely.

Keywords Privacy, Protest, Confidentiality, Mental models

Paper type Research paper

Information & Computer Security
Vol. 24 No. 4, 2016
pp. 400-415

2056-4961
DOI 10.1108/ICS-06-2015-0024

1. Introduction

Privacy is a human right in Europe, and the UK is a signatory of the European Convention of Human Rights. Article 8 of the Convention states (European Convention, 2012): *Right to respect for private and family life:*

(1) *Everyone has the right to respect for his private and family life, his home and his correspondence.*

(2) *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

The Snowden revelations about mass surveillance ought, then, to have been greeted with expressions of outrage. The response has, in reality, been muted (Paramaguru, 2013; Motherboard, 2014). We would have expected to see numerous letters to the press, online petitions and sanctions from the UK Government. However, we did not notice any of these things happening.

Privacy researchers, on the other hand, *are* concerned about computer users divulging too much information (Barnes, 2006), not appreciating or valuing their personal information and giving it away unthinkingly, thereby unwittingly sacrificing their personal privacy (Norberg *et al.*, 2007). The lack of outrage from the general public seems to confirm that people do not realise how their privacy is being violated, or, perhaps, there is another reason. The message actively promoted by intelligence agencies is that privacy needs to be sacrificed for the state to be able to protect citizens from harm (Best *et al.*, 2006; Manningham-Buller, 2012). Have people accepted this compromise to feel safe and secure?

It is instructive to look at the searches carried out on Google to assess public concern and interest. Table I shows the results of a Google News Archive query for co-located terms since the Snowden leaks in December 2014. It is interesting that "privacy" and "security" are most often searched for together, as are "privacy violation" and "security". It seems as if the public has indeed been persuaded that these two concepts are interrelated. A search for the emotive term "sacrifice" together with "privacy" and "security" for the same time period delivers only three results, and there were no searches for National Security Agency (NSA) and "protect" or for NSA and "prevent tracking", which seems rather strange.

Table I shows the number of searches but not trends over time. We can get a better impression of concern levels over time by checking whether the UK public searched for these terms before and after the revelations. Figure 1 shows the result of a Google Trends query of searches made in the UK for the words "privacy", "NSA" and "Snowden". The top line reflects searches related to privacy and shows a slight

Table I. Google News Archive search (UK only) for these co-located terms

Period 1/5/2013-28/2/2014	NSA	GCHQ	Confidential	Secret	Security	Snowden
Privacy/Private	4240/2360	2020/421	2930/1360	53600/13500	65300/20900	3730/982
Privacy violation	9	10	9	8	1410	215

downward trend since 2004. The middle and bottom lines reflect the number of searches for "NSA" and "Snowden". The peaks reflect public interest that occurred just after the leaks.

The interesting aspect of this graph is that there was no corresponding peak in searches related to "privacy". This might mean that although they registered that their government was tracking them, they did not make the mental connection to their own privacy being violated by these actions.

Preibusch (2015) examined immediate effects of the revelations and says: "I found no sustained growth in the user base of privacy-enhancing technologies" (p. 48) and "The continued reporting on state surveillance by the media contrasts with the public's quickly faded interest" (p. 50). Richter (2014) carried out an investigation into how internet users, as a whole, reacted to Snowden's revelations. He published the graph, shown in Figure 2, to demonstrate how people changed their behaviours.

Google's archives suggest that the NSA's actions excited interest, but surprisingly, people generally did not seem to link this to privacy or to violations thereof or at least did not search for these terms more often. This is curious, to say the least. The Richter (2014) chart shows changes in behaviour but does not suggest that people decided to protest. What one *does* observe is an increase in protective behaviours?

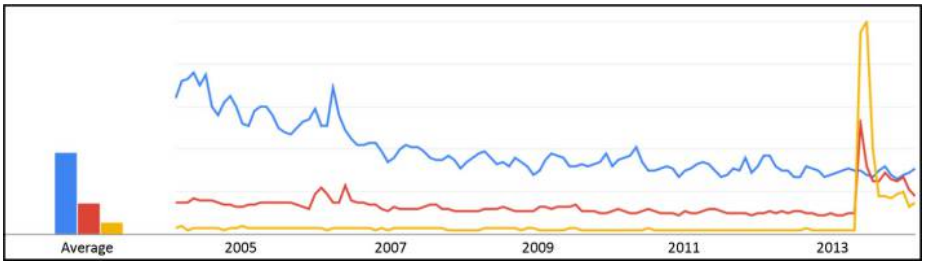

Figure 1.
Created using google.com/trends – December 2014

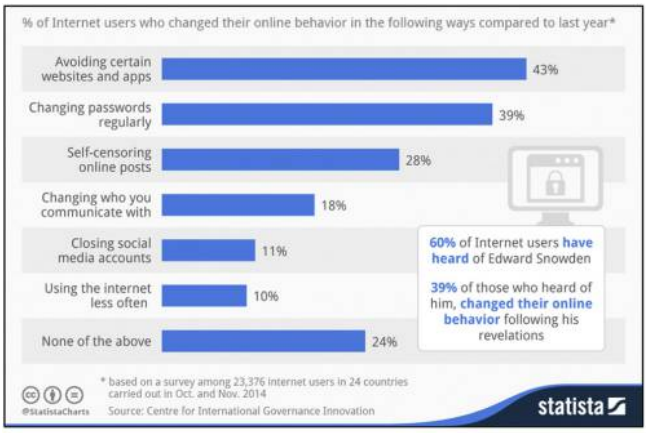

Figure 2.
How internet users adapted after Snowden revelations

Source: Richter (2014)

What about the actual protests? A Google News Archive search for *surveillance and protest* from 20 May 2013, when the revelations first broke, to December 2014, constrained to the UK, delivers a number of results. Many of these report protests in the USA. However, two UK-specific news reports about public protests in the aftermath of the Snowden revelations appear on the first page. The first, titled "Low-key GCHQ protest over surveillance case under way" (BBC, 2014), reports that protesters were outnumbered by officers and media representatives. A follow-up protest, outside GCHQ, is titled "GCHQ privacy protest descends into urine drinking after low turnout" (Merriman, 2014). This reports fewer than 100 attendees. A large-scale protest would surely generate a larger number of news reports than we found, and we have to conclude that the Snowden revelations did not lead to any significant level of protest in the UK.

The literature tells us that people generally engage in protest action because they feel aggrieved (Berkowitz, 1972; Gurr, 1970; Lind and Tyler, 1988 as cited by Klandermans and De Weerd, 2000). The Oxford English Dictionary defines a grievance as: "A real or imagined cause for complaint, especially unfair treatment". If feeling aggrieved leads to action, does that mean that the UK public does not feel aggrieved? Klandermans and Oegema (1987) proffer a four-stage process which leads to protest, the first of which is that people need to sympathise with the cause and the second that they themselves are targeted – any protest that ensues requires these two stages to occur first. Being in sympathy suggests an understanding of the source of a grievance, and being targeted suggests that the person him or herself is affected. A protest cannot occur without both of these preconditions. Other factors predicating protest are mentioned in the literature, and we will explore these later in the discussion section. For now, we want to focus on the formulation of a grievance.

Consider the first possibility: a lack of understanding. Privacy is undoubtedly a nebulous concept, and it is possible that the public does not fully comprehend the implications of the surveillance or realise that they themselves were likely to be targeted (Margulis, 1977). The second possibility is that they *did* understand that their privacy had been routinely and gratuitously violated, but because of media coverage and fear-inducing messages from intelligence bodies, they have been persuaded that security and privacy are mutually exclusive, and that they have to sacrifice privacy if they want to be secure (Koerner, 2014).

We, thus, surveyed a class of final-year bachelor's and master's students taking a security-related course. Although they were not explicitly taught the meaning of these terms, we considered that they ought to be more aware of their meaning than the general population. What we wanted to find out was whether educated students with an interest in security understood privacy and confidentiality concepts well enough to articulate and apply the principles. If even those interested in security, and well educated, did not have this understanding, then this would point to a more general lack of understanding and might explain the lack of protest. If, on the other hand, they *did* have good mental models of privacy and confidentiality, then we have to spread the net wider to understand the apparent apathy of UK citizens.

In summary, we discovered that our participants did indeed have an understanding of privacy and confidentiality such that they could categorise related scenarios correctly most of the time. On the other hand, they were not able to verbalise their understanding in the form of definitions and sometimes defined one

term in terms of the other. We report on their responses in Section 4 and discuss our findings in Section 5. Section 6 concludes.

2. Related work

2.1 Knowledge

For many years the field of information security has demonstrated a strong belief in the power of knowledge, i.e. that a lack of knowledge is responsible for sub-optimal behaviours. For example, Albrechtsen (2007) points to a lack of knowledge and motivation to explain why users do not behave securely. Stanton *et al.* (2005), too, end their paper by reporting on an investigation into end-user behaviours by saying "organizations can help to ensure that workers have the motivation and knowledge to follow the policies that the organization sets to promote its security agenda". This is an abiding theme in many publications in this research area. There is an implicit assumption that giving people the knowledge they need will automatically lead to the desired behaviour. If we apply this to the privacy arena, this should mean that if people understand their privacy rights, and are attuned to violations, they will then stand up for these and protest violations. Lately, some researchers have started to query the assumption that knowledge will automatically lead to action (Furnell, 2005; Renaud, 2012; Renaud and Goucher, 2014). These researchers do not claim that knowledge is unimportant, only that it is not sufficient to lead to action on its own. This paper seeks to contribute towards this debate in the privacy arena.

2.2 Mental models

People's understanding of complex concepts is encoded within their mental models. So, to assess understanding, we tried to gain insight into these mental models. Mental models have been studied in several other security and privacy critical contexts, such as in the context of online behavioural advertisements (Ur *et al.*, 2012); anonymous credentials (Wästlund *et al.*, 2012); photo sharing (Cunningham and Masoodian, 2010); internet use (Furnell *et al.*, 2007); firewalls (Raja *et al.*, 2011); security warnings (Bravo-Lillo *et al.*, 2011); end-to-end verifiable electronic voting (Olembo *et al.*, 2013); and mobile security (Benenson *et al.*, 2012). Wash (2010) studied mental models in security in general, as well as Camp (2009). An overview of mental model-related research in human-centred security and privacy is presented by Volkamer and Renaud (2013). In the field of information security, many studies have reported flawed or incomplete end-user mental models, leading to a poor understanding of threats and consequences. The main motivation for most of the researchers was to use mental models to base security and/or privacy communication on their new insights, be it in terms of awareness, education or improved interfaces. Our focus here is on privacy-related mental models in general to understand inaction in the face of revelations that should, at least in some citizens, have excited outrage.

Many methods for assessing mental models in this context have been proposed (Volkamer and Renaud, 2013). Some have used interviews; others ask people to depict their understanding in a drawing. We decided to use an explorative approach: first we asked the participants to define the terms, and then, on the flip side of the paper, we asked them to identify particular scenarios as being privacy, confidentiality or security violations. In doing this, we did not merely test the bottom levels of Bloom's pyramid

(Anderson *et al.*, 2001), the ability to *remember*, we also required them to *understand* and *apply* their knowledge in a given context.

2.3 The terms confidentiality and privacy

The ISO/IEC 27001 (2013) definition of confidentiality is: "that information is not made available or disclosed to unauthorized individuals, entities, or processes". The ISO/IEC 29100 (2011) provides a definition of the privacy principle: "specific choices made by a personally identifiable information (PII) principal about how their PII should be processed for a particular purpose".

Despite these standards, a number of other understandings of privacy and confidentiality manifest in the literature, especially where the man and woman in the street are likely to look.

For example, online dictionaries do not do a particularly good job of distinguishing between these terms: confidentiality and privacy. Meriam-Webster describes confidentiality as "secret or private" and privacy as "freedom from unauthorized intrusion" and "secrecy". The Oxford English Dictionary defines privacy as "a state in which one is not observed or disturbed by other people". Collins defines confidentiality as "spoken, written, or given in confidence; secret; private" and privacy as "not widely or publicly known" and "confidential".

Definitions of privacy are also frequently discussed in literature on ethics and law. For example, DeCew (1997) points out that if privacy is "not having others possess certain information", then this is equivalent to secrecy, but argues that information may be secret but not private (e.g. military strategies). Later, DeCew (1997) comments that if your phone was tapped and someone heard you ordering pizza, one would say that your privacy had been breached, yet the information is not necessarily secret. Many people unsurprisingly conflate privacy and confidentiality, probably because the information being protected is personal and sensitive in both cases. These are very different concepts because of who controls the information. Privacy, we will argue, is related to a person having the right to control his or her own information. Winslade and Ross (1985) provide a detailed analysis of privacy perceptions from different academic areas, including psychology, economics and philosophy. They concur that privacy is essentially bound up with choice, denoting an individual's right to divulge, or to grant access to, information or their own bodies.

Privacy and security are often mentioned together, as if they are somehow impossible to separate. McDaniel and McLaughlin (2009) talk about the challenges introduced by smart meters in the national grid and use the phrase "privacy and security" as a unit throughout the paper. They suggest that correct implementation of security will ensure that customer privacy is not violated. If one searches the academic literature, it seems that this is a common trend (Di Pietro and Mancini, 2003; Dourish and Anderson, 2006; Mather *et al.*, 2009). Even Internet Service Provider (ISPs) seem to follow this trend. Newman (2014) reports on a leak at Comcast and quotes the email provider as saying "[…] We take our customers' privacy and security very seriously […]".

Although privacy and security are often used together, as a mantra, some publications appear to use the terms "privacy" and "confidentiality" interchangeably. For example, Acquisti *et al.* (2006) state:

> A common motivation for organizations to invest in information security is to safeguard their confidential data as well as their customers' personal information. Over the past few years,

> privacy incidents have been announced frequently enough to question whether organizations have the necessary incentives to safeguard consumer information.

In the first sentence, the word "confidential" is used to refer to their own data, but when they talk about breaches related to customer data, it becomes "privacy". Yet, if one considers the legal definitions of these words, it seems that the word "confidentiality" should have been used in the second sentence. Yet, other publications use the words privacy and confidentiality as a pair, sometimes even joining them with a hyphen (Singer *et al.*, 2003; Rothstein, 1997; Olsen and Sabin, 2003). The media also does this. Gye and Evans (2014), reporting on police sneaking a peek at the official database to spy on ex-partners, quote Khan, the Chief Executive of Victim Support, as saying: "Victims rightly expect that their privacy and the information they give will be respected when they report a crime". Once again, the term "privacy" is used instead of the correct term: "confidentiality".

In the research literature, confidentiality refers to the duty of a third party, someone to whom a person has divulged something (Winslade and Ross, 1985). Such a third person has a duty to keep the information confidential (Anderlik and Rothstein, 2001), and this obligation is often enforced by law if the party is an organisation, especially within the European Union. Reston and Sherrer (1973) define confidentiality as a promise made by a therapist to their client about unauthorised disclosure of information. Although this relates specifically to a client/therapist relationship, a similar definition can be seen in computing science with regards to confidentiality policies in information systems. For example, Biskup and Weibert (2004) discuss confidentiality as the need to disclose certain information to only a subgroup of users and note that this can be achieved by access control or information flow control. It seems that where confidentiality is defined, it can be more cohesive, but, as discussed previously, it is often conflated with privacy.

To summarise, our review of literature leads us to conclude that privacy is "the right to decide what to divulge, and who to grant access to", the key here being the element of choice. Confidentiality, on the other hand, is a related but different concept which involves private information being divulged to a third party who has "a duty of care to protect this information and only allow access to those who have the right thereto".

3. Survey

We conducted a study to find out how well educated students understand *privacy* and *confidentiality*. We formulated a number of survey questions to evaluate the mental models of the related concepts. In setting up our survey, we were immediately confronted by the haziness of the definitions. The literature review revealed no one cohesive definition for privacy and confidentiality. Furthermore, security, which we did not ask them to define, is "the state of being free from danger or threat". We include this definition here, because we anticipated, based on the literature review, that our respondents might conflate security and privacy, so we want to be clear about what our understanding of security is. Figure 3 depicts privacy and confidentiality and their relationship.

We surveyed 46 students taking a Cyber Security course in 2014. This sample was chosen because these individuals can be expected to be well versed in the meaning of these concepts (the Cyber Security course is essentially a course about cryptography and the technical aspects of security).

The participants were asked to provide a definition for the terms, and, then, on the flip side of the page, they were presented with 15 scenarios for categorisation. These 15 scenarios, with the expected classification (based on extracting commonalities and removing conflicting concepts from the literature), are:

(1) Someone in your family finds and reads your diary (privacy violation, as the word "finds" suggests that access was not granted).

(2) You are forced to go through a full body scanner at the airport that reveals your body under your clothes (Privacy violation; the element of choice has been removed, as one has already invested money and time into this flight, and you are unlikely to refuse and, thus, be refused permission to fly).

(3) You are patted down by someone of the opposite gender at an airport (privacy violation, as one does not really have the right to decide; the same reason as the previous scenario).

(4) The NSA read your e-mails (on the network; privacy violation, as access was not granted).

(5) Paparazzi take photos of a famous individual in his or her own home through the windows (privacy violation, as we assume that access was not granted).

(6) Someone breaks into your house and steals your laptop with all your personal files on it (security violation, as we assume that this constitutes a failure of your household security).

(7) A mugger steals your smartphone from you. You have not set up a PIN or password protection on your phone (lack of personal security measures, as PINs etc. are not in place).

(8) Someone steals your identity and uses it to get a credit card (security violation, as someone compromised the mechanisms that protected the ID).

(9) Someone clones your credit card and runs up charges on your bill (security violation, as the anti-cloning mechanism has been compromised).

(10) Your neighbour is a nurse. She looks up details about your health while she is at work (to snoop on you; confidentiality violation, as curators are supposed to ensure that access is restricted to those who have been authorised to access).

(11) A government minister loses a laptop with details about your name, phone number and address on it (confidentiality violation, as the minister is supposed to protect this information).

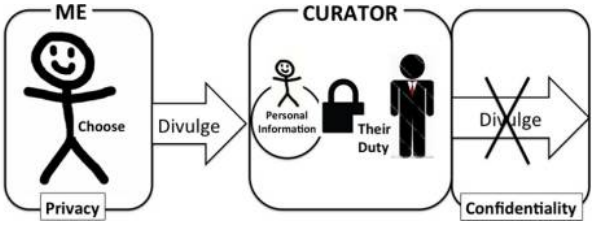

Figure 3.
Depicting privacy and confidentiality

(12) Google analyses your e-mails to target advertising more intelligently (confidentiality violation unless you know that you granted access when you signed up).

(13) A counsellor uses details of sessions with clients as examples on their website (confidentiality violation).

(14) The UK's National Health Service sells your health data (anonymised) without your permission (confidentiality violation, as they have the legal responsibility to keep the data confidential and did not explicitly ask for your permission to share your data)[1].

(15) A local nightclub requires you to provide them with your fingerprint to gain access (none, as the clubber has the choice not to enter the club without loss, and other clubs are available).

We included security scenarios to see whether the participants were able to distinguish these from privacy and confidentiality. Thus, in total we had: five privacy scenarios, four security scenarios, five confidentiality scenarios, and one scenario which we believed to be a non-issue. We are aware that the reader might not fully agree with our classification. This already confirms the fuzzy boundaries between these concepts.

4. Results – analysis

We coded the definitions and grouped these into themes – first independently then agreeing on one coding after a discussion between the researchers. In this study, 8 of the participants produced two incorrect definitions, whereas 12 produced two correct definitions. There were clear indications of confusion between individual definitions with similar semantics being used to define different terms by the same participant (Table II). In the following sub-sections, we report the themes that emerged from the definitions. Note that we will not be reporting quantitative data with respect to themes, as this is a mental models study, with all themes being equally important. We will, however, give an indication of the percentage of correct definitions overall.

4.1 Privacy definitions

A total of 21 codes emerged, with about one-fifth of definitions judged correct. The most frequent themes were "keeping information from others without sharing", which sounds more like secrecy, and "choice of disclosure of information", which does not include access to our persons as well. In those definitions that included the theme of "choice", there was mention of retaining the information unless they chose to disclose it, whereas the other theme specifically mentioned not sharing information. There were two mentions of the "right to be left alone" (Galvez-Cruz, 2009).

The most prominent themes repeat the key proposition by Winslade and Ross (1985) that privacy is bound in *choice*: the right to divulge information. However, there were some disparate themes, such as the collection, storage and use of information by others, which

Table II. Definitions using similar semantics

	Confidentiality	Security	Private, i.e. circular definition
Privacy	7	2	10
Confidentiality		11	4

align more with the concept of confidentiality. One theme was related more too physical privacy – "the *right* to do what you like in your own personal space and time". There were eight mentions of "Safe and Secret", which arguably conflates privacy with security.

One comment mentioned "dependent on context and subjective". Similarly, the same respondent noted that he believed privacy concerned individuals and not organisations. Although we agree with these comments, the aim was to construct a dictionary-like definition; as such, it was difficult to incorporate these comments.

4.2 Confidentiality definitions

A total of 20 codes emerged from the provided definitions, with about half judged partially correct. The most frequent theme was "restricted access" and "permitted entities not sharing or sharing only when necessary". They did not talk about the curator having a responsibility to secure the information. The restricted access theme was established from comments that concerned control of access, echoing the discussion of confidentiality by Biskup and Weibert (2004).

The theme of permitted entities not sharing information (or sharing only when necessary) included comments about providing information to entities who then either do not share the information or share it only under certain circumstances. The latter was only mentioned by one respondent. Hence, 21 of the 22 occurrences of the theme relate to permitted entities practicing non-disclosure. This theme echoes the non-disclosure in Reston and Sherrer (1973), though it is not restricted to a psychiatrist/client scenario. The remaining themes were much less frequent. There were themes that had occurred in or were related to secrets, safety, security of information and privacy, which confirms the confusion between terms.

4.3 Results – scenarios

For two scenarios, the majority differed from our categorisations: Scenarios 12 and 15. Scenario 12 concerned Google analysing e-mails for targeted advertising and was categorised as a privacy instead of a confidentiality issue. Scenario 15 (our contentious scenario) concerned the gathering of fingerprints for entry into a nightclub and was categorised as a privacy issue by the majority. The subtle difference that we believe is missed here by the students is the element of choice, which makes this scenario a non-issue.

Scenario 9 (credit card cloning) received 100 per cent of votes for a single categorisation. Most scenarios received a clear majority (at least twice as many votes as the next highest). However, one was close – Scenario 3. Scenario 3 concerned being patted down by a member of the opposite gender at the airport: this won by a majority of 22, but 18 believed this to be a non-issue. Also, security was indeed conflated with privacy in Scenario 2, and privacy was conflated with confidentiality in Scenario 4.

5. Discussion and protests

Our study reveals a relatively good understanding, by the participants, of what confidentiality and privacy actually mean in a particular context. This suggests that the majority of the participants had correct mental models and could apply those to given scenarios. Laufer and Wolfe (1977) explain that "Individuals' concepts of privacy are tied to concrete situations in everyday life" (p.22). So, given a scenario, they can be expected to identify privacy and confidentiality invasions correctly. Hence, according to Klandermans and Oegema's (1987) model, they should be able to sympathise with and understand the implications of wide-scale surveillance and the fact that they themselves could be targeted.

On the other hand, our participants experienced difficulty articulating their understanding. They often conflated the terms in their definitions. Gross (1967) described this conundrum very well: "Without difficulty we regularly recognise those situations in which a violation of privacy is threatened or accomplished, yet stumble when trying to make clear what privacy is". Almost 50 years later, our students manifest the same difficulty as that expressed by Gross himself.

Gross (1967) quotes Hart (1954), who says: "We can know yet not understand". This seems to conflict with Bloom's suggestion that we need to understand first before we can apply knowledge (Anderson *et al.*, 2001). Privacy is perhaps a concept that does not fit into the usual mould. Given this difficulty, two points need to be made:

- First is to question whether the participants really understood the concepts or were merely able to recognise the scenarios, which Laufer and Wolfe (1977) suggest is innate.
- Second is whether they would be able to argue coherently against privacy invasions or be able to demand that their privacy be respected, given their difficulty in formulating definitions.

We do not have answers to these questions, but our findings might well identify something that deters protest. The general public, who generally do not have the advantages of a security-specific education, are probably even less likely to be able to argue for their privacy rights.

Other factors might also have deterred protest. Here, we review a non-exhaustive selection, which seeks merely to give a flavour of the complexity of the decision process. We wish to highlight the fact that knowledge and understanding of the principles of privacy does not automatically lead to action.

McCarthy and Zald (1977) suggest that, sometimes, people do not protest because they lack the resources to do so. The UK embraces the principles of democratic protest, so there was no legal or societal deterrent, but perhaps, the resource required in this case is an ability to argue coherently to demand their privacy rights, and this does not seem to come easily to them, at least not to our participants.

Klandermans and De Weerd (2000) argue that aggrieved people will protest when they have a collective identity with others who share their sense of being treated unfairly. Could there be a lack of collective identity? Does the British public no longer feel a common identity with other residents? Palmer (2012) suggests that there are hard lines between ethnic groups in the UK, and Jaspal (2009) argues that people get their identity from their language. With the UK of 2015 being a multicultural and multilingual society, perhaps, people no longer feel that they share a common identity with others such that they consider that others are likely to share their sense of being aggrieved. This is clearly a topic for political and social scientists to explore.

Van Stekelenburg and Klandermans (2013) explain that, sometimes, people do not protest because they feel cynical about their politicians and do not feel that it will have any effect – that their protests will lack efficacy. They argue that "the more effective an individual believes protest participation is, the more likely he/she is to participate" (p. 3). This explanation might hold water in the UK, with the electorate sending a clear message to the government in the recent European elections in England, when United Kingdom Independence Party (UKIP) unexpectedly gained a majority (Wintour and Watt, 2014). Kettle (2006) claims that the British have become mistrustful of their

government and explores reasons why this should be so. These reasons are not relevant here, only the fact that many in Britain seem not to trust their politicians.

It also seems pertinent to mention the British acceptance of the widespread deployment of CCTV, even though it does not make them feel safer (Ditton, 2000). The UK has more CCTV cameras per head than any other nation on earth. Its citizens have, thus, become habituated to the idea of surveillance. As they have not objected to the CCTV cameras all over their cities, why would they object now? According to Abelson (1968), humans have a strong desire for consistency, and it might cause a feeling of cognitive dissonance (Festinger, 1962) to complain about surveillance of one type when they have meekly accepted another type of surveillance.

It seems likely that any or all of these explanations, or others that we have not included, contribute towards the apparent apathy of the British public in the face of dragnet surveillance (Figure 4). Note that knowledge and understanding are not considered a causative, contrary to intuition, given what is argued by Laufer and Wolfe (1977) and expressed so eloquently by Gross (1967). We seem to know when our privacy is being invaded: it is not something that needs to be taught. Also note that we do not mean to suggest that only one explanation might deter the UK public from protesting; it might well be a combination of more than one in reality.

The upshot is that with this variety of detours, and subsequent inaction by the electorate, the erosion of our privacy rights will continue unabated and also lead to subsequent generations having fewer privacy expectations. What they will learn to expect is what they experience, and the activities of bodies such as the NSA will no longer seem a privacy violation, but a matter of course. That will be a sad day when we realise that we have given up something priceless, *privacy*, for something unattainable, *security* (Solove, 2011).

As privacy researchers, we consider that privacy is worth protecting, yet we acknowledge that others might not share our perspective. Some may feel that privacy is an outmoded expectation in the twenty-first century (Rauhofer, 2008). They may accept the invasions that dragnet surveillance constitutes as something inevitable, a natural consequence of the march of technological progress (Sturges, 2005). Some might consider complete disclosure a natural price to be paid for the benefits we gain from ubiquitous connectivity. We have suggested a number of explanations for a lack of protest, and this perspective must also be acknowledged.

Figure 4.
To protest, or not to protest, that is the question

6. Conclusions and future work

We set out to explore whether the lack of a response to the Snowden revelations could be traced to a lack of understanding of privacy. Most of our informed participants seemed to understand what the term meant and were able to classify scenarios, but it seems that this understanding was largely subconscious or tacit. When asked to verbalise their understanding, they conflated privacy, confidentiality and security, displaying some difficulty in expressing their understanding of the concepts in a coherent definition.

As understanding of the terms is clearly not the whole story, other explanations for the lack of outrage were advanced, including mining the rich social science literature in this respect. Whatever the combination of factors that has led to a lack of protest, it seems important for us to inform the upcoming generation of the meaning of privacy and their privacy rights, enshrined in EU law. First, we need to ensure that people understand how they can be tracked and subjected to surveillance, that they have the requisite knowledge. Then, we need to act to help them to articulate their concerns, if indeed this does concern them, so that they can insist upon their rights and protest when these are violated.

Note

1. It may seem that anonymisation ensures confidentiality, but many researchers believe that the anonymisation techniques are not as effective as they should be (Kalra *et al.*, 2006).

References

Abelson, R.P. (1968), *Theories of Cognitive Consistency: A Sourcebook*, Rand McNally College Publishing Company, Chicago.

Acquisti, A. Friedman, A. and Telang, R. (2006), "Is there a cost to privacy breaches?", An Event Study, in WEIS, 26-28 June, Cambridge.

Albrechtsen, E. (2007), "A qualitative study of users' view on information security", *Computers & Security*, Vol. 26 No. 4, pp. 276-289.

Anderlik, M.R. and Rothstein, M.A. (2001), "Privacy and confidentiality of genetic information: what rules for the new science?", *Annual Review of Genomics and Human Genetics*, Vol. 2 No. 1, pp. 401-433.

Anderson, L., Krathwohl, D., Airasian, P., Cruik-Shank, K., Mayer, R., Pintrich, P., Raths, J. and Wittrock, M. (2001), *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives*, Complete Edition, L. Anderson and D. Krathwohl (Eds), Longman, New York.

Barnes, S.B. (2006), "A privacy paradox: social networking in the United States", *First Monday*, Vol. 11 No. 9.

BBC (2014), "Low-key GCHQ protest over surveillance case under way", *BBC*, 29 August.

Benenson, Z., Kroll-Peters, O. and Krupp, M. (2012), "Attitudes to IT security when using a smartphone", *IEEE Federated Conference on Computer Science and Information Systems (FedCSIS)*, *Kraków*.

Berkowitz, L. (1972), "Frustrations, comparisons, and other sources of emotion aroused as contributors to social unrest", *Journal of Social Issues*, Vol. 28 No. 1, pp. 77-92.

Best, S.J., Krueger, B.S. and Ladewig, J. (2006), "Privacy in the information age", *Public Opinion Quarterly*, Vol. 70 No. 3, pp. 375-401.

Biskup, J. and Weibert, T. (2004), "Data and applications security XXIV", *Lecture Notes in Computer Science, Confidentiality Policies for Controlled Query Evaluation*, Springer, Berlin, Heidelberg, pp. 1-13.

Bravo-Lillo, C. Cranor, L.F. Downs, J.S. and Komanduri, S. (2011), "Bridging the gap in computer security warnings: a mental model approach", *Security & Privacy*, Vol. 9 No. 2, pp. 18-26.

Camp, L.J. (2009), "Mental models of privacy and security", *Technology and Society Magazine, IEEE*, Vol. 28 No. 3, pp. 37-46.

Cunningham, S.J. and Masoodian, M. (2010), "Analyzing users' behaviour to identify their privacy concerns", paper presented at Workshop on Privacy and Usability Methods Pow-wow (PUMP), Dundee, 6 September.

DeCew, J.W. (1997), *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Cornell University Press, Ithaca and London.

Di Pietro, R. and Mancini, L.V. (2003), "Security and privacy issues of handheld and wearable wireless devices", *Communications of the ACM*, Vol. 46 No. 9, pp. 74-79.

Ditton, J. (2000), "Public attitudes towards open street CCTV in Glasgow", *British Journal of Criminology*, Vol. 40 No. 4, pp. 692-709.

Dourish, P. and Anderson, K. (2006), "Collective information practice: emploring privacy and security as social and cultural phenomena", *Human Computer Interaction*, Vol. 21 No. 3, pp. 319-342.

European Convention (2012), "Article 8 of the European convention on human rights", available at: www.equalityhumanrights.com/sites/default/files/documents/humanrights/hrr_article_8.pdf

Festinger, L. (1962), *A Theory of Cognitive Dissonance*, Vol. 2, Stanford University Press, Stanford, CA.

Furnell, S. (2005), "Why users cannot use security", *Computers & Security*, Vol. 24 No. 4, pp. 274-279.

Furnell, S., Bryant, P. and Phippen, A.D. (2007), "Assessing the security perceptions of personal Internet users", *Computers & Security*, Vol. 26 No. 5, pp. 410-417.

Galvez-Cruz, D.C. (2009), "An environment for protecting the privacy of e-shoppers", *doctoral dissertation*, University of Glasgow, Glasgow.

Gross, H. (1967), "Concept of Privacy", *The New York University Review*, Vol. 42, p. 34.

Gurr, T. (1970), *Why Men Rebel*, Princeton University Press, Princeton, NJ.

Gye, H. and Evans, S.J. (2014), "Police officers caught spying on their ex-wives, uploading illicit videos on YouTube and snooping on Liverpool captain Steven Gerrard", *The Daily Mail*, 11 February, available at: www.dailymail.co.uk/news/article-2556906/Police-officers-caught-spying-ex-wives-uploading-illicit-videos-YouTube-discussing-cases-social-media.html

Hart, H.L.A. (1954), "Definition and theory in jurisprudence", *Law Quarterly Review*, Vol. 70 No. 277, pp. 37-60.

ISO/IEC 27001 (2013), Information Security Management Systems, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), available at: www.iso.org/iso/iso27001

ISO/IEC 29100 (2011), Privacy Framework, International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), available at: www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123

Jaspal, R. (2009), "Language and social identity: a psychosocial approach", available at: www.academia.edu/200226/Language_and_social_identity_a_psychosocial_approach

Kalra, D., Gertz, R., Singleton, P. and Inskip, H.M. (2006), "Confidentiality of personal health information used for research", *The BMJ*, Vol. 333 No. 7560, pp. 196-198.

Kettle, M. (2006), "We can't just blame our lack of trust on Tony Blair's 'lies'", *The Telegraph*, available at: www.theguardian.com/commentisfree/2006/dec/30/comment.voterapathy

Klandermans, B. and De Weerd, M. (2000), "Group identification and political protest", in Stryker, S., Owens, T.J. and White, R.W. (Eds), Self, Identity, and Social Movements. University of Minnesota Press, Minneapolis, pp. 68-92.

Klandermans, B. and Oegema, D. (1987), "Potentials, networks, motivations, and barriers: steps towards participation in social movements", *American Sociological Review*, Vol. 52, pp. 519-531.

Koerner, R. (2014), "Privacy vs security: a false dichotomy", available at: www.huffingtonpost.com/robin-koerner/privacy-vs-security-a-fal_b_4698157.html

Laufer, R.S. and Wolfe, M. (1977), "Privacy as a concept and a social issue: a multidimensional developmental theory", *Journal of Social Issues*, Vol. 33 No. 3, pp. 22-42.

Lind, E.A. and Tyler, T.R. (1988), *The Social Psychology of Procedural Justice*, Plenum Press, New York, NY.

McCarthy, J.D. and Zald, M.N. (1977), "Resource mobilization and social movements: a partial theory", *American Journal of Sociology*, Vol. 82 No. 6, pp. 1212-1241.

McDaniel, P. and McLaughlin, S. (2009), "Security and privacy challenges in the smart grid", *Security & Privacy, IEEE*, Vol. 7 No. 3, pp. 75-77.

Manningham-Buller, E. (2012), *Securing Freedom*, Profile Books, London.

Margulis, S.T. (1977), "Conceptions of privacy: current status and next steps", *Journal of Social Issues*, Vol. 33 No. 3, pp. 5-21.

Mather, T., Kumaraswamy, S. and Latif, S. (2009), *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance*, O'Reilly, Sebastapol.

Merriman, C. (2014), "GCHQ privacy protest descends into urine drinking after low turnout", *The Inquirer*, 1 September.

MOTHERBOARD (2014), "As Obama speaks, why is the UK So quiet on surveillance?", 17 January, available at: http://motherboard.vice.com/blog/as-obama-speaks-why-is-the-uk-so-quiet-on-surveillance

Newman, L.H. (2014), "Comcast internet customers: you should change your password", *Future Tense*, 10 February.

Norberg, P.A. Horne, D.R. and Horne, D.A. (2007), "The privacy paradox: personal information disclosure intentions versus behaviors", *Journal of Consumer Affairs*, Vol. 41 No. 1, pp. 100-126.

Olembo, M., Bartsch, S. and Volkamer, M. (2013), "Mental models of verifiability in voting", in Steve Schneider, V.T. and Heather, J. (Eds), *VoteID13, volume 7985 of Lecture Notes in Computer Science*, Springer, Bern, pp. 142-155.

Olsen, J.C. and Sabin, B.R. (2003), "Emergency department patient perceptions of privacy and confidentiality", *The Journal of Emergency Medicine*, Vol. 25 No. 3, pp. 329-333.

Palmer, A. (2012), "Multiculturalism has left Britain with a toxic legacy", *The Telegraph*, 11 February, available at: www.telegraph.co.uk/news/uknews/immigration/9075849/Multiculturalism-has-left-Britain-with-a-toxic-legacy.html

Paramaguru, K. (2013), "Three months after Snowden's NSA revelations, Europe has moved on", *Time World*, 27 September, available at: http://world.time.com/2013/09/27/three-months-after-snowdens-nsa-revelations-europe-has-moved-on/

Preibusch, S. (2015), "Privacy behaviors after Snowden", *Communications of the ACM*, Vol. 58 No. 5, pp. 48-55.

Raja, F., Hawkey, K., Hsu, S., Wang, K.L. and Beznosov, K. (2011), "Promoting a physical security mental model for personal firewall warnings", CHI '11 Extended Abstracts on Human Factors in Computing Systems, CHI EA '11, ACM, pp. 1585-1590.

Rauhofer, J. (2008), "Privacy is dead, get over it! 1 Information privacy and the dream of a risk-free society", *Information & Communications Technology Law*, Vol. 17 No. 3, pp. 185-197.

Renaud, K. (2012), "Blaming noncompliance is too convenient: what really causes information breaches?", *Security & Privacy, IEEE*, Vol. 10 No. 3, pp. 57-63.

Renaud, K. and Goucher, W. (2014), "The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture", *Human Aspects of Information Security, Privacy, and Trust*, Springer LNCS, Crete, pp. 361-372.

Reston, R.S. and Sherrer, C.W. (1973), "Malpractice: what's new?", *Professional Psychology*, Vol. 4 No. 3, pp. 270-276.

Richter, F. (2014), "How Internet users adapted after Snowden revelations", *Statista*, 28 November, available at: www.statista.com/chart/3002/how-internet-users-adapted-after-snowden-revelations/

Rothstein, M.A. (Ed.) (1997), *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era*, Yale University Press, New Haven.

Singer, E., Van Hoewyk, J. and Neugebauer, R.J. (2003), "Attitudes and behavior: the impact of privacy and confidentiality concerns on participation in the 2000 Census", *Public Opinion Quarterly*, Vol. 67 No. 3, pp. 368-384.

Solove, D.J. (2011), *Nothing to Hide: The False Tradeoff Between Privacy and Security*, Yale University Press, New Haven and London.

Stanton, J.M., Stam, K.R. Mastrangelo, P. and Jolton, J. (2005), "Analysis of end user security behaviors", *Computers & Security*, Vol. 24 No. 2, pp. 124-133.

Sturges, P. (2005), "Is privacy dead?", *Library+ Information Update*, Vol. 4 No. 11, p. 16.

Ur, B., Leon, P.G. Cranor, L.F. Shay, R. and Wang, Y. (2012), "Smart, useful, scary, creepy: perceptions of online behavioral advertising", *SOUPS '12*, ACM, Washington.

Van Stekelenburg, J. and Klandermans, B. (2013), "The social psychology of protest", *Current Sociology*, 15 March 2013.

Volkamer, M. and Renaud, K. (2013), "Mental models - general introduction and review of their application to Human-Centred security", Lecture Notes in Computer Science, Papers in Honour of Johannes Buchmann on the Occasion of his 60th Birthday, (8260), pp. 255-280.

Wash, R. (2010), "Folk models of home computer security", *Proceedings of the Sixth Symposium on Usable Privacy and Security, SOUPS '10, ACM, Redmond, WA*, pp. 11-16.

Wästlund, E., Angulo, J. and Fischer-Hübner, S. (2012), "Evoking comprehensive mental models of anonymous credentials", NetSec'11, Springer, pp. 1-14.

Winslade, W.J. and Ross, J.W. (1985), "Privacy, confidentiality, and autonomy in psychotherapy", *Nebraska Law Review*, Vol. 64 No. 4, p. 578.

Wintour, P. and Watt, N. (2014), "UKIP wins European elections with ease to set off political earthquake", 26 May 2014, available at: www.theguardian.com/politics/2014/may/26/ukip-european-elections-political-earthquake

Further reading

Anderson, J.M. (2003), "Why we need a new definition of information security", *Computers & Security*, Vol. 22 No. 4, pp. 308-313.

About the authors

Karen Renaud is a Scottish Computing Scientist working on all aspects of Human-Centred Security and Privacy in the School of Computing Science at the University of Glasgow and is one of the five UK Cyber Security Fulbright Awardees for 2016/17. She is particularly interested in supporting innovation in security and privacy.

Dr Melanie Volkamer has been appointed Full Professor for Usable Privacy and Security at Karlstad University. She is also a Professor (Kooperationsprofessur) at the Department of Computer Science of Technische Universität Darmstadt (Germany) since August 2016. Before she was an Assistant Professor at TU Darmstadt, Professor Volkamer has been heading the research group "SECUSO – Security, Usability and Society" since 2011.

Corresponding author
Stephen Flowerday is the corresponding author and can be contacted at: sflowerday@ufh.ac.za